3/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI
(c) 2003 THOMSON DERWENT. All rts. reserv.

009750319 **Image available**
WPI Acc No: 1994-030170/ **199404**
XRPX Acc No: N94-023775
Signal encryption system for radio communications networks - uses different ciphering codes for communication between radio centre station and mobile sites in case of failure in cipher feedback mode NoAbstract
Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 5336108	A	19931217	JP 92144126	A	19920604	199404	B

Priority Applications (No Type Date): JP 92144126 A 19920604
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 5336108	A		8	H04L-009/06	

Abstract (Basic): JP 5336108 A
Dwg.5/6
Title Terms: SIGNAL; ENCRYPTION; SYSTEM; RADIO; COMMUNICATE; NETWORK; CIPHER; CODE; COMMUNICATE; RADIO; CENTRE; STATION; MOBILE; SITE; CASE; FAIL; CIPHER; FEEDBACK; MODE; NOABSTRACT
Derwent Class: W01; W02
International Patent Class (Main): H04L-009/06
International Patent Class (Additional): H04B-007/26; H04L-009/14
File Segment: EPI

3/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2003 JPO & JAPIO. All rts. reserv.

04344408 **Image available**
RADIO COMMUNICATION SYSTEM

PUB. NO.: 05-336108 [**JP 5336108** A]
PUBLISHED: December 17, 1993 (19931217)
INVENTOR(s): TSURUMI HIROSHI
OGURA KOJI
SHINPO ATSUSHI
OBAYASHI SHUICHI
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-144126 [JP 92144126]
FILED: June 04, 1992 (19920604)
INTL CLASS: [5] H04L-009/06; H04L-009/14; H04B-007/26
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems)
JOURNAL: Section: E, Section No. 1527, Vol. 18, No. 165, Pg. 36, March 18, 1994 (19940318)

ABSTRACT

PURPOSE: To make excellent ciphering, high reliability and flexible service possible by using a different ciphering to make verification when verification is not made through the use of ciphering between a radio base station and a mobile terminal equipment.

CONSTITUTION: When an ID number of its own station is sent from a radio terminal equipment 11 to a radio base station 7 and dialing is made, the radio base station 7 sends a verification request for verifying the radio terminal equipment to the radio terminal equipment 11 making dialing. A random number is generated by the radio base station 7 usually and it is

sent to the radio terminal equipment 11. The radio terminal equipment 11 uses a ciphering key of its own station to cipher the sent random number and returns the result to the radio base station 7 as a verfication acknowledge. The radio base station 7 uses a ciphering key of the radio terminal equipment in a database to cipher the random number generated in its own station and compares it with the random number sent from the radio terminal equipment 11. As the result of comparison, when the error is a prescribed error rate or below, the radio base station 7 regards as the radio terminal equipment 11 to be a legal terminal equipment and when the required reception error rate is not satisfied, the ciphering mode is changed and verification is implemented.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－336108

(43)公開日　平成５年(1993)12月17日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｈ０４Ｂ	7/26	１０９　Ｒ	7304－5K			
			7117－5K	Ｈ０４Ｌ	9/ 02	Ｚ

審査請求　未請求　請求項の数１(全　８　頁)

(21)出願番号　特願平4－144126

(22)出願日　平成４年(1992)６月４日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　鶴見　博史
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

(72)発明者　小倉　浩嗣
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

(74)代理人　弁理士　須山　佐一

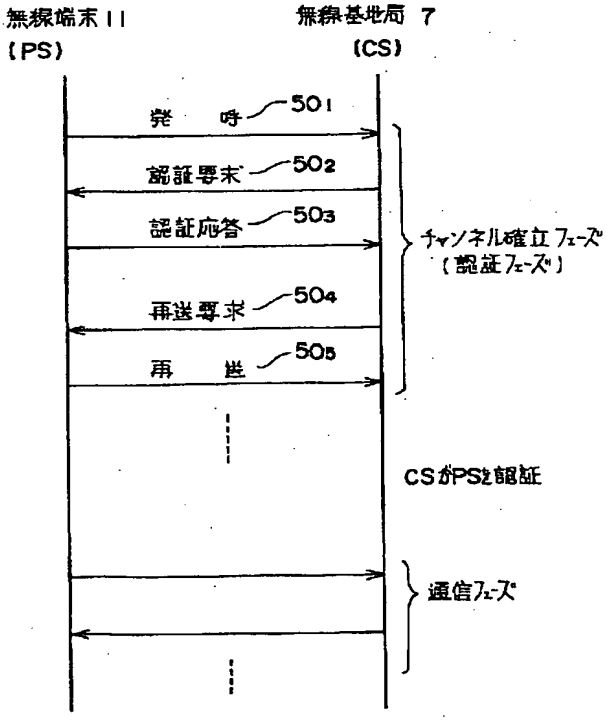
最終頁に続く

(54)【発明の名称】　無線通信システム

(57)【要約】

【構成】　ある信号モードで無線基地局７は、無線端末１１に対して認証要求を行い（ステップ５０２）、無線端末１１から認証応答が無線基地局７に送られる（ステップ５０３）。この認証が正しくない場合、無線基地局７は異なる暗号モードで無線端末１１に対して再送要求を行い（ステップ５０４）、無線端末１１から再送が行われる（ステップ５０５）。このようにして異なる暗号モードで認証が行われる。

【効果】　秘話性に優れ、信頼性が高く、柔軟なサービスを行うことができる無線通信システムを提供することができる。



1

【特許請求の範囲】

【請求項１】　無線基地局と移動体端末との間で通信を行う無線通信システムにおいて、

発呼時において無線基地局と移動体端末との間で暗号を用いて認証ができない場合、異なる暗号を用いて認証を行うことを特徴とする無線通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コードレス電話、携帯電話、自動車電話等の移動通信端末を有する無線通信システムに関するものである。

【０００２】

【従来の技術】近年、携帯電話、自動車電話等の移動通信端末を用いた無線通信システムが利用されている。このような無線通信システムでは、通信の秘匿のために暗号が利用される。

【０００３】

【発明が解決しようとする課題】ところで、かかる無線通信システムにおいては、無線区間の通信に暗号を使用していても無線区間伝送路のフェージング、シャドウイング等による受信誤りがあった場合に、受信側ではこれが伝送路誤りによる受信誤りであるのか、あるいは自端末が本来と異なる暗号鍵を使用して悪意の通信を行っているのかの区別がつかないという問題があった。

【０００４】また、送信情報の内容にかかわらず、常に単独の暗号モードを使用する場合には、端末において暗号、復号の際に処理に長時間要したり、消費電流が増す等の問題があった。

【０００５】本発明は、このような問題に鑑みてなされたもので、その目的とするところは、秘話性に優れ、信頼性が高く、柔軟なサービスを行うことができる無線通信システムを提供することにある。

【０００６】

【課題を解決するための手段】前述した目的を達成するために本発明は、無線基地局と移動体端末との間で通信を行う無線通信システムにおいて、発呼時において無線基地局と移動体端末との間で暗号を用いて認証ができない場合、異なる暗号を用いて認証を行うことを特徴とする無線通信システムである。

【０００７】

【作用】本発明では、無線基地局と移動体端末との間で暗号を用いて認証ができない場合、異なる暗号を用いて認証を行うものである。

【０００８】

【実施例】以下、図面に基づいて本発明の実施例を詳細に説明する。

【０００９】図１は、本発明の一実施例に係る無線通信システムの概略構成を示すものである。これは通常、セルラ方式と呼ばれる無線通信方式である。同図において、１は公衆網、３は無線制御局、５は同軸ケーブル、

2

光ファイバ、もしくは無線伝送路、７は無線基地局（ＣＳ）、９はセル、１１は移動無線端末（以下無線端末と称する。）を示す。そして、無線制御局３は記憶装置１３を有している。

【００１０】このような無線通信システムにおいて、各セル９内の無線端末１１は、それぞれ各セルの無線基地局７と無線を用いて通信を行う。各無線基地局７は、同軸ケーブルもしくは光ファイバ５等によって無線制御局１３によって接続されている。加入された無線端末１１や無線基地局７に関する情報は、記憶装置１３に保存される。このようなシステムで盗聴等のセキュリティー上の問題があるのは、無線端末１１と無線基地局７の間である。

【００１１】図２は、無線端末１１の構成を示すブロック図である。この無線端末１１は、アンテナ２１、無線回路２３、変復調回路２５、暗号化復号化回路２７、制御回路２９、受信電界強度検出回路３１、伝送路推定回路３３、記憶回路３５を有する。

【００１２】変復調回路２５は、信号の変調および復調を行う。暗号化復号化回路２７は、複数の暗号利用モードを内蔵し、送信すべき信号に対して暗号化を行い、また受信された信号に対して復号化を行う。制御回路２９は、各部の制御を行う。受信電界強度検出回路３１は、受信された受信電界の強度を検出する。伝送路推定回路３３は、マルチパス等を検出する。符号Ｓ１は入力装置３７から入力される局ＩＤ、暗号鍵、暗号利用モードの変更等を示す信号である。

【００１３】図３は、無線基地局７の構成を示すブロック図である。この無線基地局７は、アンテナ４１、無線回路４３、変復調回路４５、暗号化復号化回路４７、制御回路４９、受信電界強度検出回路５１、伝送路推定回路５３、記憶回路５５、インタフェース回路５７を有する。

【００１４】変復調回路４５は、信号の変調および復調を行う。暗号化復号化回路４７は、複数の暗号利用モードを内蔵し、送信すべき信号に対して暗号化を行い、また受信された信号に対して復号化を行う。制御回路４９は、各部の制御を行う。受信電界強度検出回路５１は、受信された受信電界の強度を検出する。伝送路推定回路５３は、マルチパス等を検出する。インタフェース回路５７は、無線制御局３とのインタフェースを行う。

【００１５】図４は、無線端末１１と無線基地局７との間で行われる暗号通信を示す図である。データＡは、暗号化復号化回路２７により暗号化され、変復調回路２５により誤り訂正符号がかけられ、無線回路２３から送信される。受信側の無線基地局７では、無線回路４３により受信され、変復調回路４５により無線伝送路で生じたビット誤りが訂正され、暗号化復号化回路４７により暗号の復号が行われる。通常、暗号・復号は、トランスペアレントな伝送路を前提としているため、暗号化を行っ

た後で、復号化を行う前に、誤り訂正を行い、通信路等で生じるビット誤りをなくしておく必要がある。ただし、無線伝送路の状態がフェージング等の影響で劣悪な場合には、誤り訂正を行ってもビット誤りは完全に訂正し切れないことがある。

【００１６】次に本実施例で用いらる暗号について述べる。暗号には大きく分けて、公開鍵暗号と慣用暗号の２通りがある。このうち公開鍵暗号は、秘匿性が高く、鍵の管理も簡単であるという利点があるが、処理時間が多く、消費電力が多いという問題点があり、低消費電力が望まれる移動通信端末用としては、慣用暗号が用いられる。この慣用暗号としては、“ISO International Standard 8372 : Information Prcessing-Modes of Operation for a 64-bit Block Cipher Algorithm”に記載されているように、ＥＣＢモード、ＣＢＣモード、ＣＦＢモード、ＯＦＢモードの４種類の利用モードが知られている。これらのモードを使用する際に問題となるのは、主に次の３点である。

【００１７】（１）鍵を固定したとき、同じ平文のデータは同一暗号文として出力される。

（２）伝送路で誤りが発生した場合には、復号後に誤り波及効果が出る。

【００１８】（３）復号化の際に、フレーム同期、ブロック同期が必要となる。

【００１９】ＥＣＢモードは、基本的な利用モードであり、上記（１）、（２）、（３）の問題があり、伝送路誤りの多い無線通信システムでの適用には不向きである。ＣＢＣモードは、上記（１）の問題は解決され、（２）に対しても、伝送路誤りは、誤りのあった直後の２ブロックにしか波及しないという特徴がある。ＣＦＢモードは、上記の問題の（３）について、同期はずれに強いという利点がある。ＯＦＢモードは、（１）を解決し、さらに（２）についても。伝送路の１ビット誤りが１ビットの復号誤りにしかならないという特徴がある。通常、雑音の多い伝送路では、２ビットの誤りが後に波及しないＯＦＢモードの適用が考えられる。

【００２０】図５は、本実施例における通信シーケンスを示す図である。

【００２１】無線端末１１（ＰＳ）と無線基地局７（ＣＳ）との間で行われる認証手順は、ＥＣＢモードを使用して行われる。すなわち、無線端末１１から自局のＩＤ番号が無線基地局７に送られ発呼が行われると（ステップ５０１）、無線基地局７は、発呼のあった無線端末１１に対して無線端末認証のための認証要求を送る（ステップ５０２）。通常は無線基地局７側で乱数が発生されて、これが無線端末１１に送られる。

【００２２】無線端末１１では、自局の暗号鍵を用いて送られてきた乱数を暗号化し、認証応答として無線基地局７に送る（ステップ５０３）。無線基地局７では、データベースにある無線端末の暗号鍵で自局で発生した乱数を暗号化し、無線端末１１から送られてきたものと比較する（ステップＢ）。

【００２３】通常、無線通信では、伝送路においてフェージング、シャドウイング、マルチパス等により受信誤りが発生する。この時、ステップ５０３のフェーズの伝送路上で誤りが発生すると、ステップＢのフェーズで受信側の復号器出力が元の平文と異なるものとなる。しかし、ステップＢで無線基地局が比較するのは、自局で発生した乱数を暗号化したものと、無線端末から送られてきたものであるので、たとえ暗号利用モードがＥＣＢモードであっても、ビット誤りは伝送路で生じたビット誤りだけで、いわゆるＥＣＢモードの誤り波及効果は出ない。ただし、ＥＣＢモードでは無線基地局から送信される乱数（チャレンジ文）自体に誤りが生じた場合には、無線基地局側で復号後に誤りが拡散する。したがって、チャレンジ文に誤り訂正を強くかければＥＣＢモードでも良いが、一般には、誤りが拡散しないＯＦＢモードの方が良いと考えられる。

【００２４】図６は、この時の処理を示すものである。まず最初に、ＯＦＢモードで暗号の通信が行われる。すなわち、無線基地局７から６４ビットの乱数Ｍを、無線端末１１に送信する。無線端末１１では、乱数Ｍに対して自局の暗号鍵Ｅｋ を用いて暗号化を行い（Ｃ＝Ek^{OFB}（Ｍ））、無線基地局７に送り返す。無線基地局７では、送られてきたＣを復号して（Ｍ＝Dk^{OFB}（Ｃ））、無線基地局７に送信した暗号Ｍと比較する。もしくは、無線基地局７の秘密鍵を用いてＭを暗号化して（Ｃ＝Ek^{OFB}（Ｍ））、送られてきたＣと比較することによって認証を行う。　無線基地局７→無線端末１１、無線端末１１→無線基地局７のいずれの伝送路で伝送路誤りがあっても、誤り波及効果はない。なお、この操作は、ＯＦＢモードの代わりに、非線形フィードバックレジスタによるストリーム暗号によって成されてもよい。

【００２５】比較の結果、２つが完全に同一であるかもしくは所定の誤り率以下であれば、無線基地局７は無線端末１１を正当な端末と見なす。ここで言う所定の誤り率とは、音声データ送信時の所要受信誤り率、例えば10^{-2}～10^{-3}に設定される。無線端末１１が偽端末の場合には、使用している鍵が異なるため、無線端末１１で暗号化され送信されてきたデータは、無線基地局７が発生した乱数を暗号化したものと全く異なる。

【００２６】この所要受信誤り率を満足していない場合には、認証に続く音声データの伝送品質が保証されないので、無線基地局７から認証の再送要求がなされ（ステップ５０４）無線端末１１から認証応答が再送される（ステップ５０５）。すなわち、この場合、暗号モードを変えて、例えば、ＥＣＢモードにて認証を行う。

【００２７】図７はこのときの処理を示すもので、ＥＣＢモードでは、無線端末１１と無線基地局７に共通の既

知データＭを持たせておき、無線端末１１がＣ＝Ek ECB（Ｍ）なる暗号化を行い、無線既知局７に送信する。無線既知局７は、自局にあるデータＭからＣ＝Ek ECB（Ｍ）を生成し、無線端末１１から送られてきたものと比較する。この方法を用いれば、ＥＣＢモードであってもビット誤りは伝送路で生じたビット誤りだけで、いわゆるＥＣＢモードの誤り波及効果は出ず、誤りは伝送路誤りに一致する。しかし、既知データＭが毎回同じである場合、伝送路上のＣを蓄積し、これを再送することにより、第三者であっても認証に成功するので、Ｍを送信の度に変える必要があり、これは例えば送受時のカウント（count ）を用いてＭ＝ｆ（count, PS-ID, CS-ID ）によって作成する。

【００２８】このように、暗号モードを変えて数回認証手続きを行っても、正当な端末と認証されない場合には、無線基地局７は無線端末１１に対して警告信号の送信、回線切断、特殊信号の送信等により、無線端末１１のＲＯＭの消去等の操作を実施する。

【００２９】なお、認証用データの受信誤り率と、既知ビットを測定して得た受信誤り率の２つを比較し、認証用データの受信誤り率が既知ビットを測定して得た受信誤り率と同程度かそれ以下であれば、誤りは伝送路で生じたものであって、無線端末１１で不正な鍵による暗号化が行われたものではないとして、無線端末１１を正当なものと認めるようにしてもよい。

【００３０】正当な無線端末と認証された場合には通信フェーズへ入る。以下、この通信フェーズについて述べる。

【００３１】この通信フェーズでは、基本的に伝送路のビット誤りが波及しないＯＦＢモード、もしくは処理時間消費電流の点で有利な周波数スクランブルや、非線形フィードバックシフトレジスタを利用したストリーム暗号を使用して伝送が行われる。　この通信フェーズにおいて、伝送する情報の内容、伝送路の状況によって、使用する暗号利用モードを適宜変更する。

【００３２】通信フェーズにおいて、制御情報や端末ＩＤ、課金情報等の重要なデータは、１ビットたりとも誤りなく伝送することが望ましいが、無線通信システムの場合、劣悪な伝送路状態のため、適宜ＡＲＱを行う必要がある。本実施例においては、このような送信情報に対してはＥＣＢモードで伝送を行う。

【００３３】ＯＦＢモードでは、受信誤りを許容できない重要な情報部分に伝送路でビット誤りを生じていても、誤り波及効果がないので、復号出力の誤り数は伝送路でのビット誤り数と対応している。したがって、重要な情報部分に誤りを生じても、暗号ブロック内の既知ビットやデータフォーマットに誤り波及が及ばない可能性があり、重要な情報部分の誤りを見逃す可能性がある。

【００３４】これに対して、ＥＣＢモードを使用した伝送では、伝送路での１ビット誤りが復号後受信情報全体に波及するため、既知ビットや送信データのデータフォーマットを観測することによって、重要な情報部分に誤りが生じていることを知ることができる。この方法では、ＣＲＣ等の冗長ビットを付加することなく、制御信号部分の誤りを検出できる。

【００３５】前述したように、音声通話時、データ送信時、制御信号送信時、認証信号送信時等、伝送する情報の内容に応じて暗号モードを選択する操作は、無線基地局７の要求によって自動的に選択される。もしくは、データ送信時に無線端末１１の使用者からの要求によって、無線端末１１の入力装置３７によって選択する。もしくは、無線端末１１に音声データ識別装置を設け、予め定められたプログラムに従って自動的に選択できるようにしてもよい。

【００３６】なお、データ伝送中においても、随時交信中の相手端末の認証を行うことがセキュリティー上望ましい。本実施例においては、無線端末１１もしくは無線基地局７からの要求によって、ＯＦＢモードを暗号利用モードとし、無線端末１１および無線基地局７間で既知データ系列の送受信を行う。ＯＦＢモードでは、伝送路の誤りが暗号復号後の誤りとなるため、データ系列を観測することにより、受信誤りの検出を行うことができる。すなわち、無線基地局７および無線端末１１内の受信電界強度検出回路３１、５１によって検出された受信レベルと、受信誤り率とを記憶回路３５、５５に記憶されている電界強度対受信誤り率データとを参照することにより、受信電界強度が受信器の受信感度レベルよりも十分に高いにもかかわらず、受信誤りが生じている場合には、交信中の端末を偽端末と判定する。

【００３７】ここで、受信電界強度が受信器の受信感度レベルよりも十分に高いにもかかわらず、受信誤りが生じている場合、交信中の端末が偽端末であるという以外に、例えば伝送路で生じるマルチパスの影響を受けていることが考えられる。これは、マルチパスの影響でビット落ちや偽ビット挿入が生じ、ブロック同期が不可能になっているからである。このような場合、無線基地局７、無線端末１１からの要求によって、同期はずれに強い１ビットＣＦＢモードの使用要求を行う。１ビットＣＦＢモードでは、このような同期はずれから抜け出す能力を備えているので、このモードを選択することによって、受信誤りが同期はずれによる誤りであるか、、あるいは交信中の端末が偽端末であるかを判定することもできる。　また、再送要求を行う場合、暗号利用モードの変更は、無線基地局７からの要求によって自動的に設定してもよいし、無線端末１１で暗号利用モードを入力装置３７によって変更できるようにしてもよい。

【００３８】かくして本実施例では、信頼性のある通信が可能で、柔軟なサービスが提供できる。

【００３９】以上、無線基地局７から無線端末１１を認証する場合について説明したが、逆に無線端末１１から

7

無線基地局７を認証することも必要となる。

【００４０】すなわち、近年、携帯電話、テレポイント等に見られるように、周波数の有効利用と、端末の小形化に伴うバッテリーの寿命の問題から送信電力を押さえるために、従来よりもさらにセル半径を小さくした、いわゆるマイクロセル方式が主体となってきている。従来、無線基地局は、サービス事業者の建物の屋上等に設置されてきていたが、極小ゾーンにおいては、基地局の大きさは、小形のものとなり、設置場所が増すことによって、必ずしも全ての基地局が、サービス事業者の目の行き届く場所に設置されるとは限らないような状況が多くなることが予想される。このような無線基地局は、従来の無線通信システムでは考えられなかった、盗難、改造、さらには子局端末の情報を盗み出すための装置として悪用される恐れが出てくる。このような理由から、無線端末１１から無線基地局７を認証する必要性が出てくる。無線端末１１から無線基地局７を認証する場合には、前述した手順を逆にすればよい。

【００４１】

【発明の効果】以上、詳細に説明したように本発明によれば、秘話性に優れ、信頼性が高く、柔軟なサービスを行うことができる無線通信システムを提供することができる。

【図面の簡単な説明】

8

【図１】　本発明の一実施例に係る無線通信システムの概略構成を示す図

【図２】　無線端末１１の構成を示すブロック図

【図３】　無線基地局７の構成を示すブロック図

【図４】　無線端末１１と無線基地局７との間で行われる暗号通信を示す図

【図５】　無線基地局７と無線端末１１との間の通信シーケンスを示す図

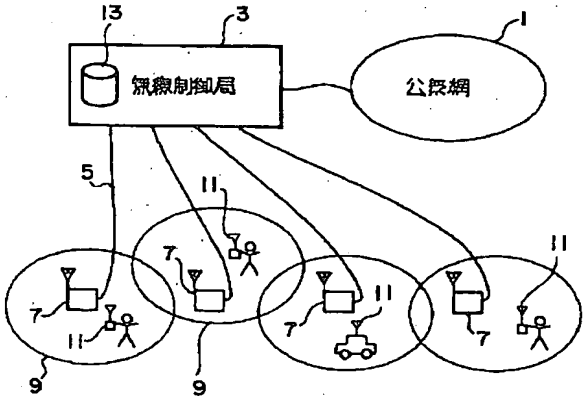
【図６】　ＯＦＢモードによる通信シーケンスを示す図

【図７】　ＥＣＢモードによる通信シーケンスを示す図

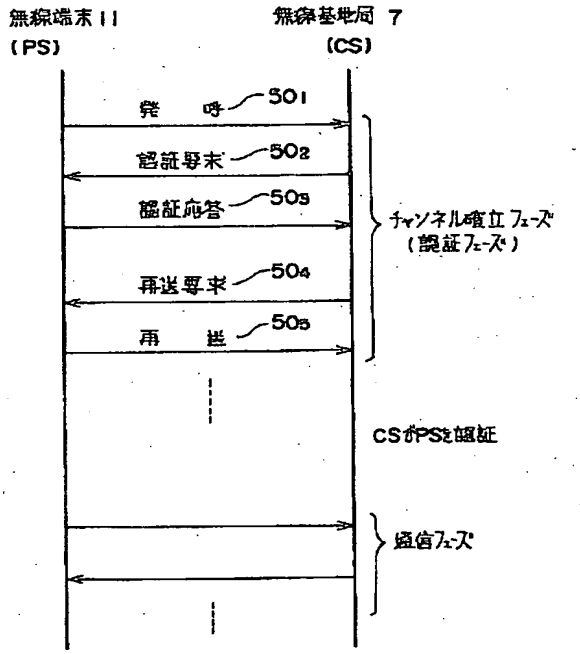
【符号の説明】

１……公衆網
３……無線制御局
７……無線基地局
１１……無線端末
２１、４１……アンテナ
２３、４３……無線回路
２５、４５……変復調回路
２７、４７……暗号化復号化回路
２９、４９……制御回路
３１、５１……受信電界強度検出回路
３３、５３……伝送路推定回路
３５、５５……記憶回路

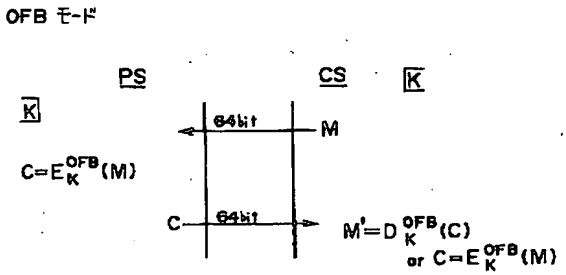
【図１】



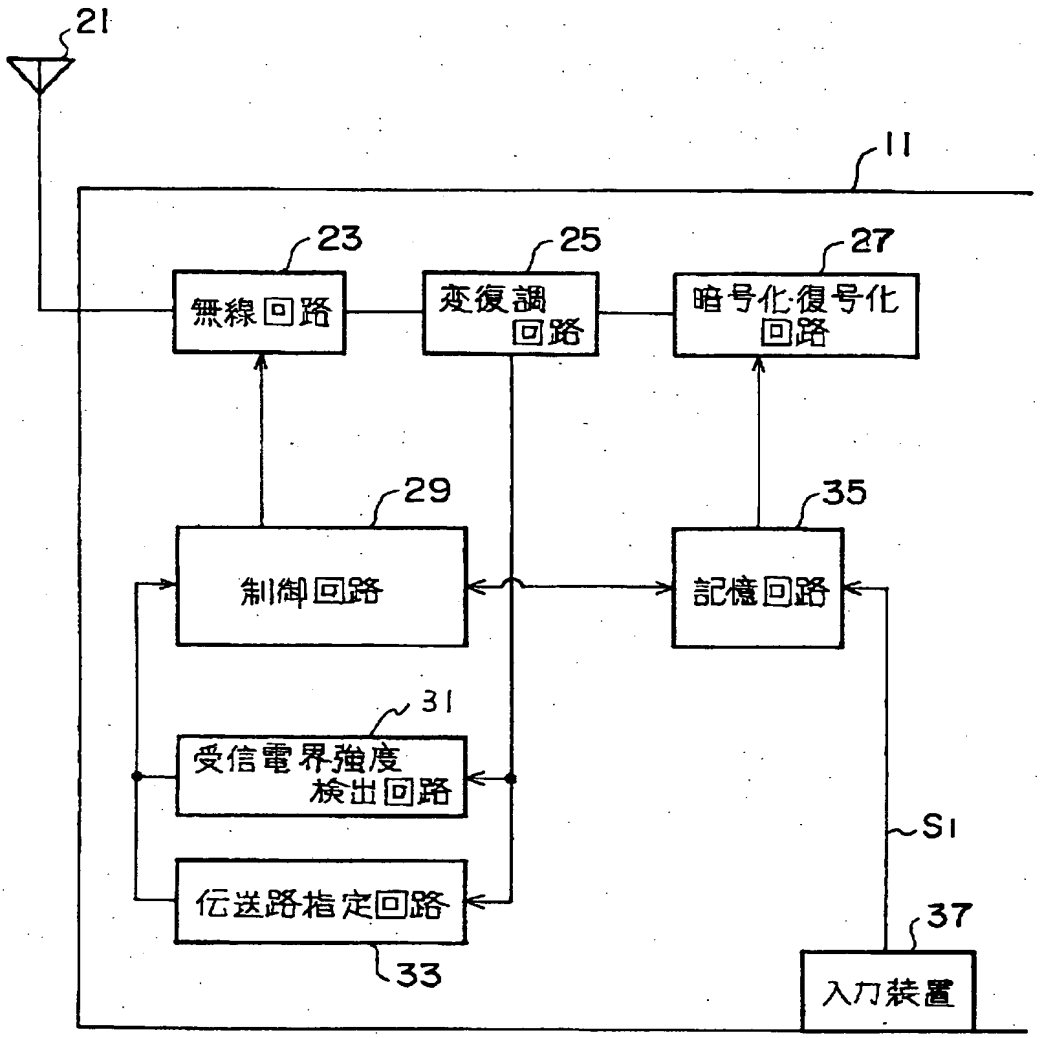
【図５】



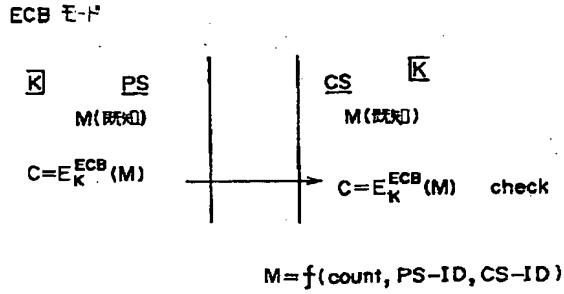
【図６】



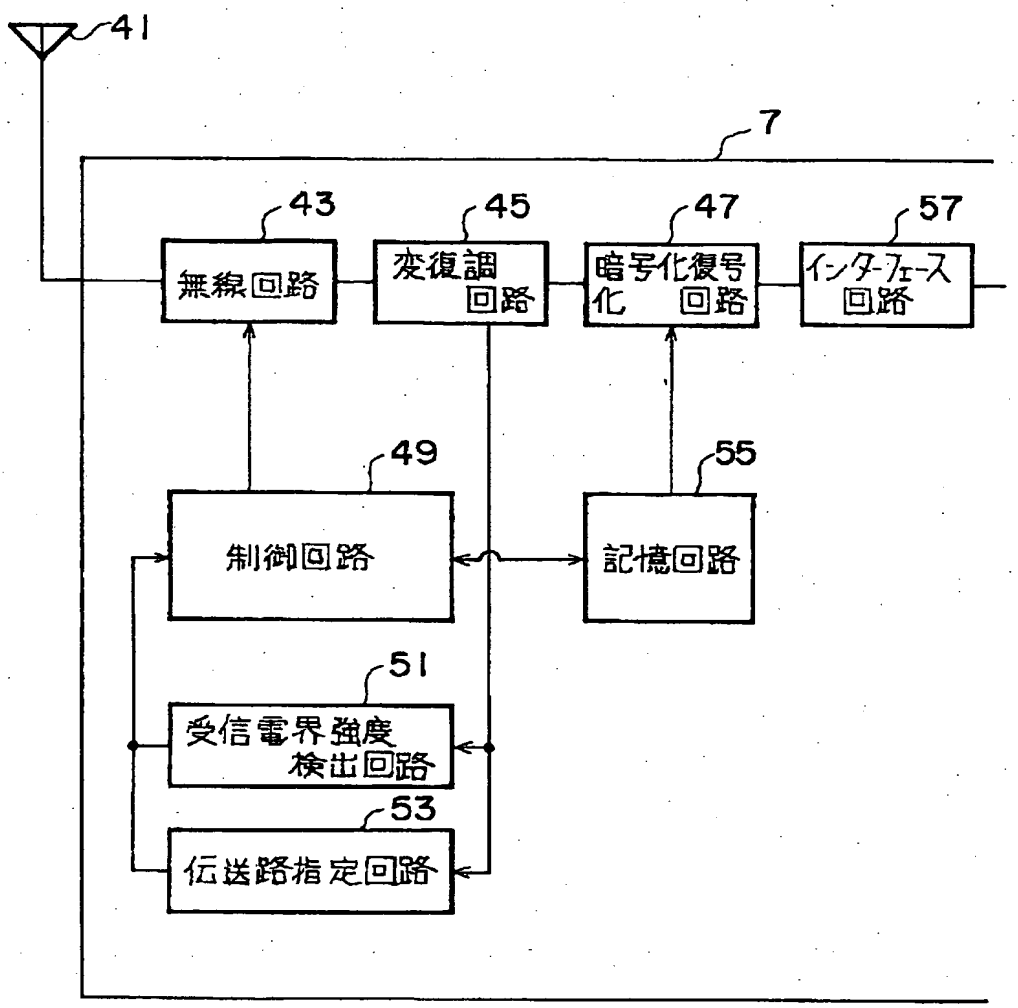
【図２】


21
11
23
無線回路
25
変復調回路
27
暗号化復号化回路
29
制御回路
35
記憶回路
31
受信電界強度検出回路
S1
伝送路指定回路
37
入力装置
33

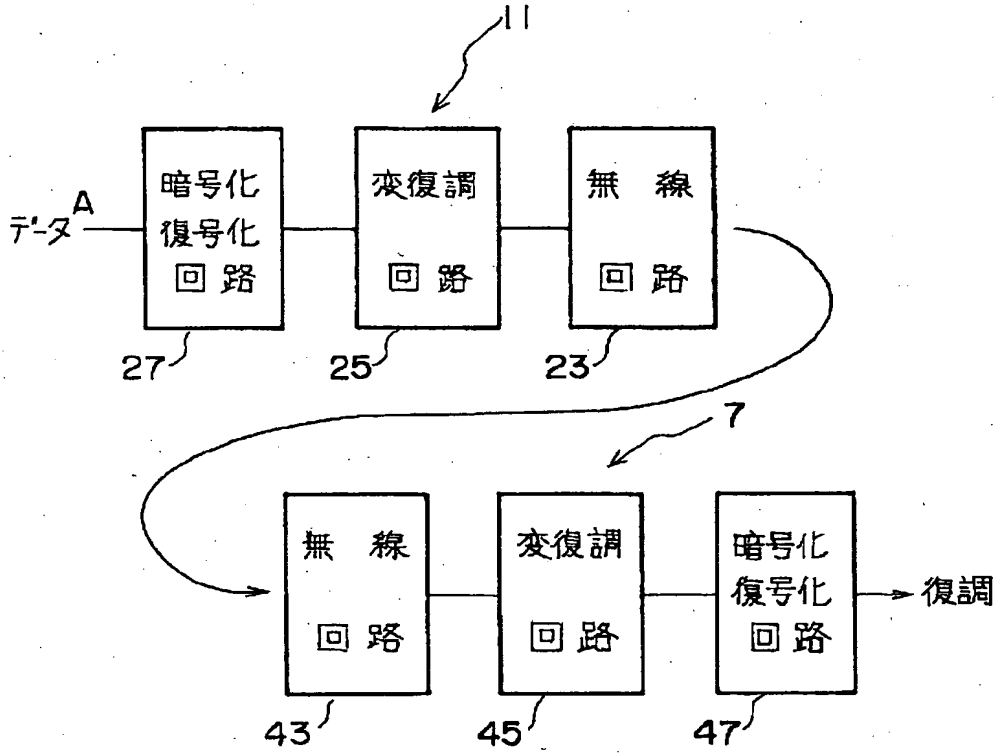
【図７】


ECB モード
K
PS
M(既知)
C=E_K^ECB(M)
CS
K
M(既知)
C=E_K^ECB(M)
check
M=f(count, PS-ID, CS-ID)

【図３】


41
7
43
45
47
57
無線回路
変復調回路
暗号化復号化　回路
インターフェース回路
49
55
制御回路
記憶回路
51
受信電界強度検出回路
53
伝送路指定回路

【図４】



フロントページの続き

(72)発明者　尾林　秀一
神奈川県川崎市幸区小向東芝町１番地　株
式会社東芝総合研究所内